APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/485,759	02/15/2000	JORDAN J. GLOGAU	3220-60866	2173

23643	7590	05/07/2004

BARNES & THORNBURG
11 SOUTH MERIDIAN
INDIANAPOLIS, IN 46204

EXAMINER
DINH, MINH

ART UNIT	PAPER NUMBER
2132	6

DATE MAILED: 05/07/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application	Applicant(s)
Office Action Summary	09/485,759	GLOGAU ET AL.
	Examiner	**Art Unit**	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>*06 February 2004*</u>.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
    closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,6-16,19 and 21-28* is/are rejected.

7)☒ Claim(s) *4,5,17,18,20 and 29* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
    application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
   Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____.
5)☐ Notice of Informal Patent Application (PTO-152)
6)☐ Other: _____.

DETAILED ACTION

Response to Amendment

1.   This action is in response to the amendment filed 02/06/2004 that amended

claims 1 and 7.

Response to Arguments

2.   Applicant's arguments with respect to claims 1-10 have been considered but are

moot in view of the new ground(s) of rejection.

3.   Applicant's arguments, see page 9, lines 1-7, filed 02/06/2004, with respect to

the rejection(s) of claim(s) 11-18 and 25-29; and page 11, lines 19-22, with respect to

the rejection(s) of claim(s) 19-22, have been fully considered and are persuasive.

Therefore, the rejection has been withdrawn. However, a discovery of new prior art has

necessitated new grounds of rejection. The delay in citation of the newly discovered

prior art is regretted.

4.   Applicant's arguments, see page 10, lines 11-15, filed 02/06/2004, with respect to

the rejection(s) of claims 23-24 have been fully considered but they are not persuasive.

Applicant points out that Podilchuk et al. do not teach sending the signal including the

hidden data to a receiving location where the message is extracted from the signal

including the hidden data. Podilchuk does teach a watermark encoder (figure 1) which

handles sending a signal including hidden data, and a watermark decoder (figure 1),

which handles receiving the signal and extracting the hidden data and any message

conveyed by the hidden data.

Drawings

5.　　The drawings are objected to because: suitable descriptive legends are required

for figures 3 and 4.　A proposed drawing correction or corrected drawings are required

in reply to the Office action to avoid abandonment of the application.　The objection to

the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

6.　　The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7.　　Claims 21 and 22 are rejected under 35 U.S.C. 112, first paragraph, as failing to

comply with the enablement requirement.　The claim(s) contains subject matter which

was not described in the specification in such a way as to enable one skilled in the art to

which it pertains, or with which it is most nearly connected, to make and/or use the

invention. The claimed invention teaches performing an exclusive-OR of the first portion

of the signal with the second portion of the signal, and performing an exclusive-OR of

encrypted message with the first portion of the signal (limitation of the parent claim,

claim 20). By doing that, the original value of the second portion of the signal must be saved so that it can be used later to recover the first portion of the signal, which in turn, is used to recover the encrypted message. The disclosure teaches embedding an exclusive-ORred value of the first portion of the signal with a value of an m-sequence into the second portion of the signal (page 8, lines 6-11); however, it does not teach saving the original value of second portion of the signal. Thus, the disclosure fails to enable one skilled in the art to make and use the claimed invention.

8.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9.   Claims 14 and 26 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The metes and bounds of the limitation "substantially random" is not clear.

Claim Rejections - 35 USC § 102

10.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent; and
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section

351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

11.   Claim 19 is rejected under 35 U.S.C. 102(e) as being anticipated by Barton

(5,912,972). Barton discloses a method comprising the steps of:

embedding an encrypted message into a first portion of a carrier signal (col. 6,

lines 57-60; col. 7, lines 16-18 and 33); and

embedding information regarding the beginning of a scan line or a frame, which

meets the limitation of message extraction information, into a second portion of the

carrier signal for extracting the encrypted message from the first portion of the carrier

signal (col. 9, line 55 - col. 10, lines 2, 9-14, 25-47).

12.   Claim 23 is rejected under 35 U.S.C. 102(a) as being anticipated by Podilchuk et

al. (Digital Image Watermarking Using Visual Models). Podilchuk discloses a method

comprising the steps of:

generating a signal including hidden data by transforming a carrier signal from a

first domain into a second domain, embedding a message into the carrier signal in the

second domain (figure 1, "Watermark Encoder");

sending the signal including hidden data to a receiving location (figure 1); and

obtaining the message from the signal including hidden data at the receiving

location by transforming the signal including hidden data into the second domain and

extracting the message (figure 1, "Watermark Decoder").

Podilchuk does not explicitly teach transforming the carrier signal back from the

second domain to the first domain. However, this feature is deemed to be inherent as

figure 1 shows that frequency decomposition is performed by the watermark decoder.

Claim Rejections - 35 USC § 103

13.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

14.   Claims 1-3, 6-8 and 25-28 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Veldhuis et al. (EP 0 359 325 A1) in view of Nakamura et al. (A

Unified Coding Method of Dithered Image and Text Data Using Micropatterns) and

Hardy et al. (5,195,136).

a.   Regarding claims 1, which is representative of claims 25 and 28, Veldhuis

discloses a method comprising the steps of:

providing a message (col. 1, line 6);

providing a carrier signal that conveys information unrelated to the message (col.

1, lines 1-5; col. 2, lines 21-24); and

embedding the message into the carrier signal by performing an exclusive-OR of

the message with a first portion of the carrier signal (col. 3, lines 1-7).

Veldhuis does not teach that the message is encrypted before it is embedded into the carrier signal. Nakamura teaches that a message is encrypted before it is embedded into the carrier signal (figure 7). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Veldhuis such that the message is encrypted before it is embedded into the carrier signal, as taught by Nakamura, so that only the receiver who has the proper key can recover both imagery and the data (see Section 6, Encryption of Text Data).

Veldhuis does not teach the steps of: generating an encryption sequence based on an encryption key and generating an encrypted message based on the message and the encryption sequence. Hardy teaches a method for data encryption, transmission, reception and decryption comprising the steps of: generating an encryption sequence based on an encryption key (figure 3), generating an encrypted message based on the message and the encryption sequence (figure 3), transmitting the encrypted message (figure 2), receiving and decrypting the encrypted message (figure 2). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the method of Hardy into the combined method of Veldhuis and Nakamura as discussed above such that an encryption sequence is generated using an encryption key and the message is encrypted using the encryption sequence. The motivation for doing so would have been to provide minimal errors in the decrypted data for each error occurring in transmission (see col. 2, lines 28-34).

b.   Regarding claim 2, Veldhuis does not disclose that the carrier signal is a digital image. Nakamura discloses that that the carrier signal is a digital image (figure 7). It

would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Veldhuis such that that the carrier signal is a digital image, as taught by Nakamura, so that the message could easily be embedded for transmission along with a digital image (see Section 6, Encryption of Text Data).

c.   Regarding claim 3, Veldhuis further discloses that first portion of the carrier signal is an LSB plane (col. 7, lines 6-11).

d.   Regarding claim 6, Veldhuis further discloses the steps of transmitting the composite signal to a receiving location, extracting the encrypted message from the composite signal at the receiving location (figure 3). Hardy further discloses the step of decrypting the encrypted message at the receiving location (figure 2, element 255).

e.   Regarding claims 7 and 27, Hardy further discloses that the step of generating an encrypted message includes performing an exclusive-OR of the message with the encrypting sequence to generate the encrypted message (col. 4, lines 53-54).

f.   Regarding claim 8, Veldhuis further discloses the steps of transmitting the composite signal to a receiving location, extracting the encrypted message from the composite signal at the receiving location (figure 3). Hardy further discloses the step of decrypting the encrypted message at the receiving location based on the encryption key (figure 2, element 255).

g.   Regarding claim 26, the limitation "substantially random" is interpreted as pseudo-random. Hardy further discloses that the encryption sequence generator is configured to generate a pseudo-random encryption sequence (col. 3, lines 61-63).

15.   Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Veldhuis,

Nakamura and Hardy as applied to claim 1 above, and further in view of Dorenbos

(5,751,813). Veldhuis, Nakamura and Hardy do not disclose that the message to be

encrypted is a pre-encrypted message. Dorenbos discloses encrypting a pre-encrypted

message (col. 2, lines 15-23). It would have been obvious to one of ordinary skill in the

art at the time the invention was made to modify the method of Veldhuis, Nakamura and

Hardy such that that the message to be encrypted is a pre-encrypted message, as

taught by Dorenbos. The motivation for doing so would have been to utilize an

encryption server when a user wishes to send a single message to multiple recipients.

16.   Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over

Veldhuis, Nakamura, Hardy and Dorenbos as applied to claim 9 above, and further in

view of Schneier ("Applied Cryptography"). Veldhuis, Nakamura and Hardy do not

disclose the step of exchanging an encryption key for decrypting the pre-encrypted

message using a trusted third party. Schneier discloses exchanging encryption keys for

decrypting an encrypted message using a trusted third party (page 185-186). It would

have been obvious to one of ordinary skill in the art at the time the invention was made

to modify the method of Veldhuis, Nakamura, Hardy and Dorenbos to include the step

of exchanging an encryption key for decrypting the encrypted message using a trusted

third party, as taught by Schneier, in order to thwart attempts to substitute one key for

another.

17.   Claims 11, 13-16 is rejected under 35 U.S.C. 103(a) as being unpatentable over

Veldhuis in view of Henry (4,471,164).

a.   Regarding claim 11, Veldhuis discloses a method comprising the steps of:

providing a message (col. 1, line 6);

providing a carrier signal that conveys information unrelated to the message (col.

1, lines 1-5; col. 2, lines 21-24); and

embedding the message into the carrier signal (col. 3, lines 1-7).

Veldhuis does not disclose that the message is an encryption sequence

generated based on an encryption key. Henry discloses a message comprising a filter

key sequence generated based on a seed (col. 3, lines 28-31, 45-54; col. 4, lines 16-

21), which meets the limitation of an encryption sequence generated based on an

encryption key. It would have been obvious to one of ordinary skill in the art at the time

the invention was made to modify the method of Veldhuis such that the message is an

encryption sequence generated based on an encryption key, as taught by Henry, so

that the receiver initialization could be accomplished.

b.   Regarding claim 13, Veldhuis further discloses that the carrier signal is an audio

signal (col. 3, lines 39-42).

c.   Regarding claim 14, the limitation "substantially random" is interpreted as

random. Veldhuis does not disclose that the encryption sequence is random. Henry

discloses that that the encryption sequence is random (col. 3, lines 30-31). It would

have been obvious to one of ordinary skill in the art at the time the invention was made

to modify the method of Veldhuis such that the encryption sequence is random, as taught by Henry, so that its outcome could not be easily predicted.

d.   Regarding claim 15, Veldhuis does not disclose that the encryption sequence is generated based on a linear feedback shift register. Henry discloses that the encryption sequence is generated based on a linear feedback shift register (col. 3, lines 45-54). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Veldhuis such that the encryption sequence is generated based on a linear feedback shift register, as taught by Henry, so that only a small portion of the sequence is necessary to initialize the sequence generator.

e.   Regarding claim 16, Veldhuis further discloses that the step of embedding the encryption sequence includes performing an exclusive-OR of the encryption sequence with a portion of the carrier signal (col. 3, lines 1-7).

18.   Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Veldhuis in view of Henry as applied to claim 11 above, and further in view of Schneier. Veldhuis and Henry do not disclose that the encryption key is a public key for an asymmetric system. Schneier discloses an encryption key being a public key for an asymmetric system (page 31, fourth paragraph). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Veldhuis such that the encryption key is a public key for an asymmetric system, as taught by Schneier, in order to solve the key-management problem with symmetric cryptosystems (page 32, first paragraph).

19.   Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over

Podilchuk as applied to claim 23 above, and further in view of Nakamura. Podilchuk

does not teach the steps of encrypting the message prior to generating the signal

including hidden data and decrypting the message after obtaining the message from the

signal including hidden data. Nakamura teaches encrypting a message prior to

generating a signal including hidden data and decrypting the message after obtaining

the message from the signal including hidden data (figure 7). It would have been

obvious to one of ordinary skill in the art at the time the invention was made to modify

the method of Veldhuis to include the steps of encrypting the message prior to

generating the signal including hidden data and decrypting the message after obtaining

the message from the signal including hidden data, as taught by Nakamura, so that only

the receiver who has the proper key can recover both imagery and the data (see

Section 6, Encryption of Text Data).

Allowable Subject Matter

20.   Claims 4-5, 17-18, 20 and 29 would be allowable if rewritten to overcome the

rejection(s) under 35 U.S.C. 112, second paragraph, set forth in this Office action and to

include all of the limitations of the base claim and any intervening claims.

21.   The following is a statement of reasons for the indication of allowable subject

matter.

a.   Regarding claims 4-5, the feature of the claim, embedding the first portion of the carrier signal into a second portion of the carrier signal, in combination with limitations of the parent claims have not been taught by prior art.

b.   Regarding claims 17-18, the feature of the claim, transmitting the encryption sequence to a receiving location and generating an encryption key at the receiving location, in combination with limitations of the parent claim have not been taught by prior art.

c.   Regarding claim 20, the feature of the claim, performing an exclusive-OR of the encrypted message with the first portion of the carrier signal, in combination with limitations of the parent claim have not been taught by prior art.

d.   Regarding claim 29, the feature of the claim, replace a first LSB plane of the digital image with information based on a second LSB plane of the digital image and to perform an exclusive-OR of the encrypted message with the second LSB plane of the digital image, in combination with limitations of the parent claim have not been taught by prior art.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 703-306-5617. The examiner can normally be reached on Mon - Fri: 9:00 am - 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.
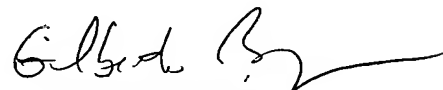
Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

MD
04/29/2004

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100